silo
By Authentic8

FLASH REPORT

Using the Dark Web in Financial Crime Investigations

The Dark Web: Designed for Anonymity

Unlike the surface web (where information is indexed and openly searchable) or even the deep web (where users are typically required to register, log in or pay to access the data not otherwise available through traditional browsers), the dark web is a labyrinth of servers and sites that diligently guard users' anonymity and encrypt all communication. When users access the dark web, their connection requests bounce around from an entry/guard node through at least three different relays until they reach the final destination: an exit node. Additional layers of obfuscation make it harder to identify the user and pinpoint their IP addresses.

Financial crime investigators are aware of the bounty of potentially valuable research data available on the dark web, but the fact that Tor was designed specifically for anonymous communications — with more than 6,000 relay nodes owned by volunteer organizations around the world — makes searching for clues and tracking leads around the Tor network an extremely daunting task. Dark web marketplaces and other sites are constantly changing, with their names and URL disappearing from view, only to be relaunched at a different location, adding to the frustration of researchers trying to investigate them or take them down.

The Criminals are Watching

While financial crime investigators are looking into potential criminal activity, the criminals are also watching them, looking for opportunities to expose agents and circumvent their missions by unmasking identities of organizations they are affiliated with. For analysts and law enforcement agents who research criminal activity on the dark web, being uncovered by adversaries can negate months — sometimes years — of careful profiling and evidence gathering.

Here are some of the ways that dark web site owners can figure out who you are:

HTML5 Canvas Fingerprinting

This technique is based on the fact that each computer and browser are unique in a way they display information. The image format depends on many factors, including hardware, software, operating system, fonts, setting, image export and compression options and many others. While the differences in how images are rendered are slight, almost imperceptible to a human eye, dark web operators can use these minute variations to fingerprint each visitor on their site. Initially, it may not reveal a fraud investigator's identity, but over time your adversaries can collect enough data points to figure out who you are based on the sites you visit, which topics you're interested in and which other users you interact with.

Researchers need to be aware that no matter how careful they are, using a regular browser to access the dark web will inevitably leave behind a trail of breadcrumbs in a form of unique and persistent canvas fingerprints, creating an opportunity for adversities to track them down.

In the late 1990s, the U.S. Department of Defense launched an anonymous network as a way for their intelligence agents to communicate clandestinely, outside of an open web. The network was later opened to other traffic to create background noise, allowing spy communication to blend in with other ongoing activity. Today, The Onion Router or, as it's more commonly known, Tor network is the technology behind the dark web – a shadowy place on the internet, which is used for both good (think free speech in areas under totalitarian government control) and evil (some analysts estimate that 60 percent of all listings refer to illegal goods and services).

JavaScript Embeds

Websites can embed code that you can't see unless you specifically look for it. And even when researchers are technical enough to identify these embeds, they can't analyze every page they visit to see if something snuck into their computer to execute commands in the background to try and gather information on their identity and location.

Accessing Personal Websites While on Tor Exit Node and Accidentally Giving out Personal Details

Sometimes criminals don't need to resort to hacking to get the information they want. A researcher who checks personal email or logs into their social media account while on a Tor exit node is risking exposing their true identity by having their surface web activity linked to their dark web browsing. A simple search can help a criminal find out which topics the researcher is looking into and whom they might be investigating. The same goes for analysts who frequent dark web forums — sometimes even experienced researchers can give out too much information, leading to their missions being compromised.

Useful Information You Can Find on the Dark Web

Digging for clues on the dark web is not easy, but for a researcher who knows where to look, it can lead to a treasure trove of valuable data. Here are some examples:

Personal Data for Sale

Passports, IDs, birth dates, driver's license numbers — these are among the most common merchandise for sale on the dark web. Most go for a small price — from a few pennies to $10 per record — and are used for a variety of nefarious purposes, including doxing, extortion and fraud. Sometimes these records are published on the dark web for free as a way for hackers to gain credibility in their circles, stir chaos, have a bit of fun or perhaps as retaliation against certain companies or individuals.

For fraud researchers, these databases can yield some useful information. For instance, a person's birthplace is often used as a security question to verify their identity for access to their financial accounts. Knowing which stolen data is for sale and cross-referencing it with your organization's client list can help sort out which customers' information might be stolen and whose accounts might be in jeopardy for unauthorized access.

Dark Web Marketplace Ads with Geotags

Geotags are metadata used to add a geographical location to images, videos, websites, QR codes and other objects on the web. Unlike open web social media sites — which strip all metadata, including location, from an image when you upload it — the dark web doesn't automatically do it, leaving some images with geolocation data intact. This information can be used by investigators to locate places where photos were taken, and ultimately uncover the identity of a seller who is using these images to advertise their (illegal) merchandize.

Simple (or Reused) Usernames and Avatars

People are creatures of habit, and we tend to reuse our usernames, passwords and avatars in both open and dark web, or create usernames that make it easy to guess our real names. There are plenty of examples of careless criminals whose simple usernames (and the fact that they asked for weapons illegally purchased on AlphaBay to be delivered to their home address) made it possible for investigators to figure out their identities.

Policies and Tools for Accessing the Dark Web

Before researchers can safely venture into the dark web, they need a clear set of guidelines from their organization that spell out exactly when they are allowed to visit the dark web sites; under what conditions can be provide payment for access; and how can they do it without compromising the safety of their corporate networks.

Safe Browsing

Traditional browsers download content from the web onto local endpoints before rendering the information on the user's screen. If a researcher accesses questionable content, or even accidentally clicks on a malicious link, they can inadvertently bring malware into their company's networks. Many researchers rely on VPN as the way to obscure their location, but with VPNs, the web code is still executing on the endpoint, exposing computers to potential threats. Researchers need safe tools that separate their browsing environment from actual machines and networks, removing the threat of malware, embedded code, and other tools that adversities use to track or threaten them.

Managed Attribution

VPNs, private browsing options, or "Do Not Track" settings — while somewhat useful — don't completely hide researchers' identities, especially from more technologically savvy, advanced adversaries. In fact, the use of a "Do Not Track" mode on a browser may signal to a criminal that a user has something to hide, and that's not what an analyst wants to do. If anything, their best bet to protect their identity and not arouse suspicion is to blend in with their surroundings. A specialized managed attribution solution helps researchers have full control over online identities, including creating and maintaining their personas, affiliations and locations.

Auditability

For any type of research, maintaining a chain of custody for all evidence is indispensable. It helps research teams reconstruct the chain of events by retracing their steps, especially in the world of the dark web, where websites disappear, and marketplaces rearrange themselves on a regular basis. Auditability and oversight are essential elements for OSINT research, as they help simplify compliance and improve case documentation for risk management teams.

The dark web is a murky place, designed primarily to conceal the identity of its users. And while gaining access to the data hosted within its shadowy depths can give investigators a powerful source of information, organizations need to design a careful access strategy to avoid potential exposure and exploits. They also need to equip their analysts with the right set of tools built specifically for safe and anonymous investigations.

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.